REMARKS

Applicant notes the Examiner's new grounds for rejecting claims 1 and 3 to 13 under 35 U.S.C. s103(a) based on the combination of Casey et al (US6493349) and Boden et al (US6832322). Reconsideration is requested.

Independent claims 1 and 13 have been amended to clarify that "wherein the NAT is arranged to map an external network address of an entity in the external network to an internal VPN address within an address range of a respective VPN". Basis for this change is found in claim 1 as originally filed, and at page 10, lines 34 to 36 and at page 12, lines 8 to 10 of the specification as filed.

Consideration of the content of Casey and, in particular, figure 2, column 3, lines 27 to 56, column 4, lines 8 to 56 and column 5, lines 4 to 28 reveals that Casey does **once** mention use of a network address translator 'NAT' function (column 5, line 17), but one that comprises traditional NAT functionality where the VPN IP source addresses are mapped to external IP source addresses for outbound traffic, but said destination IP addresses are also external IP addresses. The NAT as taught by Casey does not map an external network address of an entity in the external network to an internal VPN address within an address range of a respective VPN as claimed.

In contrast to Casey, independent claims 1 and 13 define a NAT that performs source and destination network address translation advantageously allowing an entity in the external network, e.g. a network resource such as a call server or a trunk gateway, to appear as though it were a resource within the VPN with an address in the VPN (e.g. an enterprise private IP address space). The NAT does this by mapping an external network address of an entity in the external network to an internal VPN address within an address range of a respective VPN. As such, the entity has a VPN IP destination address in contrast to Casey where such an entity only has an external destination IP address.

No reason exists to modify Casey in the manner suggested by the Examiner. Furthermore, in order to modify the system of Casey to arrive at that claimed, it would be necessary to go against the teaching of Casey as regards the use of network address translation since Casey clearly and unambiguously teaches that entities in the external network(s) have source and destination addresses within the external network(s). In any event, to modify Casey in the manner asserted by the Examiner would require much more than merely supposedly using a source and destination NAT of a type as allegedly taught by Boden. It would require that all of said entities taught by Casey as existing in the external networks and clearly disclosed as having external network addresses would have to have internal VPN network addresses assigned to them and then to arrange the NAT to map said external addresses to the assigned internal addresses in the respective address ranges of respective VPNs. It is noted that the Examiner overlooks the practical implications of his broad assertion that one skilled in the art would contemplate modifying Casey to use a NAT as taught by Boden, notwithstanding the fact that there is no reason why one skilled in the art would contemplate doing so.

The Examiner acknowledges that Casey does not *explicitly* show where the NAT comprises source and destination. For the record, it is noted that the Examiner does not argue that Casey somehow *implicitly* discloses this feature and applicant strongly asserts that there is neither explicit nor implicit disclosure of this feature in Casey.

The Examiner looks to Boden as providing evidence of the well known feature of using a NAT comprising source and destination, although it is not clear from the Examiner's comments precisely what he construes a "NAT comprising source and destination" as comprising.

In any event, Casey is unambiguously directed to providing VPN service by allowing <u>partitioning</u> of (large) VPNs into smaller areas, isolating the topology complexity of those areas and interconnecting them using (virtual) routers, essentially creating a hierarchy. This does not lend itself to using a VPN gateway and NAT arrangement as claimed and it is submitted that, for the rejection to stand, the Examiner must explain why one skilled in the art would ignore the teaching of Casey when attempting to modify it to apply a NAT of the type allegedly disclosed by Boden.

<u>Casey mentions NAT in only one place (c.5 l.17)</u>. The NAT as mentioned by Casey is used to allow the VPN to break out to external networks (e.g. the Internet), performing *standard* NAT functionality. The NAT in Casey translates the internal VPN addresses (typically private IP

addressing used by enterprises) to public IP addresses to connect with external resources on the public networks using the public addresses of those external resources (i.e. a packet outbound from the VPN to an external resources as a destination IP address that is the public IP address of the external resource).

In applicant's application, specific external resources are made available to the VPN by having the VPN gateway NAT map the public addresses of the specific external resources to corresponding addresses of respective VPNs (e.g. using VPN private IP addresses).

It is important to note that Boden describes the use of IPSec to provide VPN and discloses specific techniques to make IPSec connections and NAT compatible. Boden describes various IP address manipulations to do so, including substituting a destination address with a substitute address. Boden specifically uses destination address substitution when interconnecting sub-networks (fig 2 Network A & B) over a shared network 460 to form a VPN where the IP addressing scheme in the interconnected sub-networks use overlapping IP addresses (as could happen with IP private address schemes). However, Boden fails to describe how multiple VPN gateways could be provided by one shared entity (the VPN gateway as claimed) and provide the type of destination address translation disclosed and claimed in the present application.

Consequently, the combination of Casey and Boden or the combination of Casey with the art evidenced by Boden fails to disclose at least one essential feature of the claimed invention and thus fails to render obvious the network efficiency that a shared VPN gateway with source and destination address translation can provide to a public network provider offering VPN services. The foregoing combination also fails to render obvious the simplification of address provision, firewall administration, security verification that results from the claimed arrangement of using a VPN gateway having a NAT shared by a plurality of VPNs in the manner claimed.

Applicant also submits that combining Casey and Boden or Casey and the art evidenced by Boden in an attempt to arrive at the claimed arrangement is non-trivial given the further significant modifications that would be required of Casey following the modification to use a NAT as taught by Boden (in the unlikely event that one skilled in the art would even have contemplated doing so, which applicant asserts he would not).

For these reasons, it is respectfully submitted that the claimed invention makes a useful contribution to the art which is non-obvious over the prior art of record.

The rejection of the dependent claims is moot in view of the above.

Favorable reconsideration of the application is requested.

June 4, 2009

Respectfully submitted,
William M. Lee
William M. Lee, Jr.
Registration No. 26935
Barnes & Thornburg LLP
P.O. Box 2786
Chicago, Illinois 60690-2786
(312) 214-4800
(312) 759-5646 – Fax